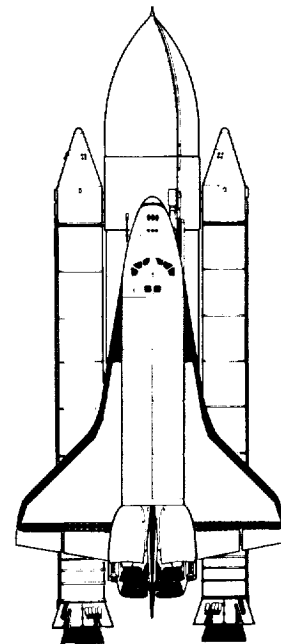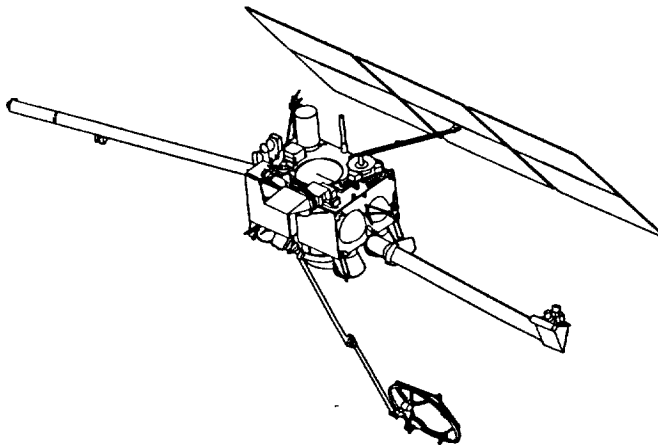# An Improved Approach for Flight Readiness Assessment

Methodology Summary

N.R. Moore
D.H. Ebbeler
M. Creager

October 30, 1990

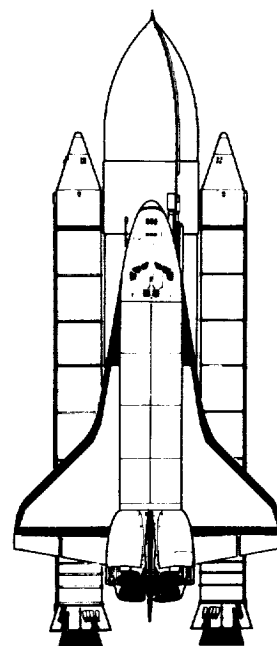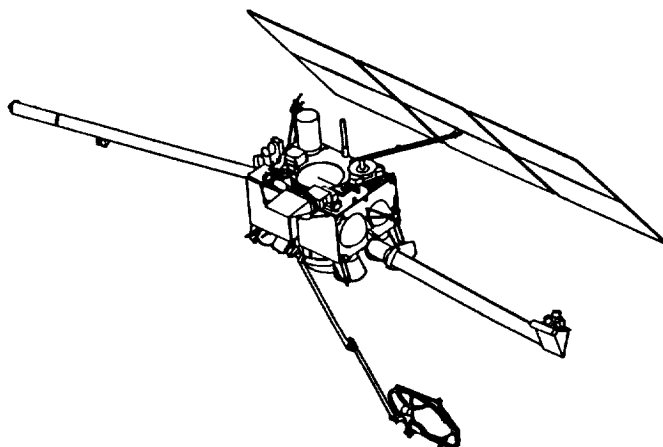# An Improved Approach for Flight Readiness Assessment

Methodology Summary

N.R. Moore
D.H. Ebbeler
M. Creager

October 30, 1990

Preface

This report presents an overview and summary of the methodology for flight readiness assessment of spaceflight systems developed by the Jet Propulsion Laboratory under NASA RTOP 553-02-01 sponsored by the Office of Space Flight, NASA Headquarters. This methodology was developed as a part of the Certification Process Assessment task carried out for the Space Shuttle Main Engine. A comprehensive report detailing the methodology, computer software, and examples of application will be formally issued in fiscal year 1991.

Acknowledgment

Abstract

An improved methodology for quantitatively evaluating failure risk for a spaceflight system in order to assess flight readiness is presented. This methodology is of particular value when information relevant to failure prediction, including test experience and knowledge of parameters used in engineering analyses of failure phenomena, is limited. In this approach, engineering analysis models that characterize specific failure modes based on the physics and mechanics of the failure phenomena are used in a prescribed probabilistic structure to generate a failure probability distribution that is modified by test and flight experience in a Bayesian statistical procedure. The probabilistic structure and statistical methodology are generally applicable to any failure mode for which quantitative engineering analysis can be employed to characterize the failure phenomenon and are particularly well suited for use under the constraints on information availability that are typical of such spaceflight systems as the Space Shuttle and planetary spacecraft.

Contents

Introduction

The occurrence of critical failures of such spaceflight systems as the Space Shuttle and planetary spacecraft must be established as extremely unlikely before missions are flown. Practices used in the aerospace community for establishing the expectation of reliable mission operation have employed a judgmental evaluation based on limited test experience and deterministic engineering analysis. Discussions of approaches to failure prediction used in the Space Shuttle program are given in [1-3]. These approaches become arbitrary and are subject to serious misinterpretation when applicable experience and information used in engineering analysis are inadequate. Moreover, testing to establish high reliability is rarely feasible for flight hardware. A discussion of the need for improved approaches for characterizing and managing failure risk, including comments on the approach presented here, is given in [2]. Because of information limitations encountered in assessing failure risk for the Space Shuttle and other spaceflight systems, such improved approaches for managing risk must be based on methods which enable the incorporation of information from both operating experience *and* engineering analysis.

Operating experience and engineering analysis, including the analysis of past experience, are the two fundamental information sources on which to base any assessment of the occurrence of failures. For certain failure modes of the Space Shuttle propulsion system, directly applicable past experience is sparse; testing sufficient to establish high reliability is infeasible; and consistently conservative engineering analyses are not meaningful. Under these conditions, a quantitative assessment of failure risk that incorporates all the available information is required to make rational decisions in managing risk.

This report presents an approach for assessing failure risk that uses information from engineering analyses and from operating experience in a statistical structure within which uncertainties of the engineering analyses and uncertainty due to limited operating experience are both quantitatively treated. This approach can be applied to any failure mode which can be described by quantitative models of the physics and mechanics of the failure phenomena. Examples of failure modes that can be quantitatively modeled include high-cycle fatigue, low-cycle fatigue, flaw propagation, stress rupture, seal leakage, and bearing wear. This approach is presented in more detail in [4].

A probabilistic assessment of failure risk is appropriate for certain failure modes of components whose failure margins are of concern. That concern usually arises because the information about the parameters that characterize a failure is limited and/or the analytical models for the failure phenomenon are approximate. Under such circumstances, probabilistic analyses are required to characterize meaningfully the conditions and service limits under which failure risk is acceptable. Probabilistic analyses are required for only a subset of the failure modes identified by means of Failure Modes and Effects Analysis (FMEA). Most of the failure modes identified by a FMEA can be shown, by means other than probabilistic analysis of the type presented here, to be extremely unlikely.

1

Presently Used Approaches to Flight Readiness Assessment

The process by which the expectation of reliable mission operation is established is referred to as certification[1] of flight readiness. More definitively, certification of a system intended for use in a specific application is the process by which confidence is established that the system will perform as expected over a specified range of environmental and operating conditions. Certification of launch vehicle propulsion systems has typically consisted of a limited amount of *certification testing* of flight configuration systems and *deterministic engineering analysis*. The deterministic engineering analysis may incorporate limited information from measurements of governing physical parameters taken during development testing.

Certification Testing

Certification testing of the Space Shuttle Main Engine (SSME) has consisted of testing two engines each under simulated mission conditions for twice the operating time or number of missions for which flight readiness is being certified, a practice commonly referred to as the *2X rule*. Under this rule, certification for a five-mission increment, for example, would consist of testing two engines each for ten missions with inspections and maintenance, including scheduled component replacement, according to procedures prescribed for flight engines. Certification is accomplished if the testing is completed with no failures or anomalous events.

Similar certification testing rules are found in past aircraft practice in both the commercial and military sectors, as exemplified by the now obsolete FAR 33.14-6 [5]. Such arbitrary factor rules for certification testing represent heuristic practices that have no formal rationale based on statistics or engineering analysis. Under credible statistical assumptions, procedures such as the *2X rule* taken alone do not provide enough operating experience to establish with high confidence that a quantitative failure probability is sufficiently low to warrant certification of flight readiness. Test programs are structured to reveal major inadequacies in design. Testing sufficient to establish high reliability at an acceptable confidence level is rarely performed for launch vehicle propulsion systems.

The value of test experience in establishing low failure probability with high confidence for flight configuration systems is limited because testing is usually halted before failures are expected to occur. For highly reliable systems, testing sufficient to encounter failures would be prohibitively time consuming and costly. Moreover, testing is normally planned to avoid failures that could result in the loss of costly hardware and damage to expensive test facilities.

As a rule, failure experience is not applicable to flight hardware because failure modes discovered during development testing are corrected by design changes which are intended to render their occurrence highly unlikely during subsequent tests and flights. Consequently, test experience for launch vehicle propulsion systems generally does not include failure data for flight configuration hardware, but instead consists of *zero-failure* test data.

The exclusive use of zero-failure tests to establish with high confidence that failure risk is low requires extensive test data. If each mission simulation test is assumed to be an identical independent trial with constant probability of failure, over 690 mission simulation tests would have to be conducted in order to have even 50 percent probability of observing a failure mode whose probability of occurrence during a mission is 1/1000.

---

[1]The term *qualification* is also used.

Deterministic Engineering Analysis

Consistently and verifiably conservative deterministic analyses to predict failure can provide assurance that the conditions under which a critical failure mode could occur do not intersect conditions that exist during mission operation. Such analyses are appropriate for most of the failure modes identified in a FMEA. In that situation, the deterministic approach serves to establish that the occurrence of the failure mode in question is extremely unlikely, although no quantitative estimate of the probability of failure is available from such analyses. When constraints and requirements for performance, weight, and cost force a departure from consistently conservative deterministic analyses for certain failure modes, worst-case or limiting values for parameters that govern failure are not always employed.

When worst-case values for the parameters that govern failure cannot be consistently used, deterministic analysis methods are credible if they are calibrated by means of past experience that is directly relevant in terms of knowledge of governing parameters, the stochastic nature of materials behavior, the accuracy of engineering models under the conditions of application, and the variability of manufacturing processes. Where there exists an extensive, directly relevant base of experience to guide the selection of less conservative safety factors and values for governing parameters, deterministic analyses provide failure predictions that are generally consistent with the experience base, although the extent of conservatism is not known.

Launch vehicle propulsion systems are typically subject to some significant number of failure modes for which important governing parameters may not be well known (e.g., knowledge of structural loads or a local environment may be highly uncertain) and the accuracy of engineering models used to characterize the failure phenomena may be in question. For certain failure modes of such systems as the SSME, where performance, weight, and cost requirements force the use of new design approaches, advanced materials, and more severe operating conditions, no suitably extensive experience base is available to calibrate deterministic analyses to characterize and predict failure.

Deterministic analyses under conditions of limited information and uncertain knowledge become arbitrary and can yield results that are subject to serious misinterpretation [1]. In these situations, a formal procedure for quantitatively accounting for risk due to limited information and uncertain knowledge is required if consistent criteria for flight readiness are to be established. In these cases, the consideration of risk by means of qualitative judgments based on deterministic analyses of failure modes and limited test experience is inadequate.

Failure Risk Assessment

At any time in the development and operation of a launch vehicle propulsion system, the available information on which to base an assessment of failure risk or flight readiness comes from two fundamental sources: engineering analysis and operating experience. Figure 1 shows how these two information sources are used in quantitatively assessing failure risk in a Bayesian statistical framework. The Bayesian statistical framework used here is a straightforward approach for combining information from engineering analysis with observed operating experience and can be applied individually to certain failure modes identified in a FMEA.
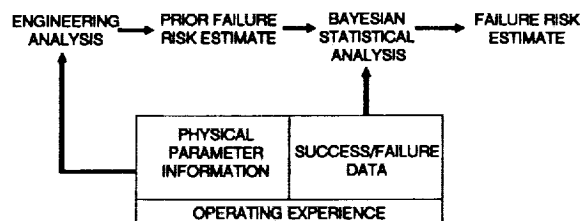
Figure 1. Information Sources for Failure Risk Assessment

Engineering analyses characterize the conditions under which specific failure modes may be expected to occur, e.g., pressure or accumulated time in service. As illustrated in Fig. 1, engineering analysis provides information to establish the *prior* failure risk estimate, called a prior distribution, which is modified to reflect available success/failure data in the Bayesian statistical analysis [6]. Engineering analysis to predict failure is based on available knowledge of governing physical parameters, e.g., loads and materials properties, that can be derived from measurements taken during operation, from past experience and analyses performed to characterize parameter values, from subsystem and component testing, and/or from laboratory tests.

As shown in Fig. 1, operating experience consists of parameter information and success/failure data. Success/failure data can be acquired from development testing, certification testing, and, possibly, flight operation. When the success/failure data for flight configuration hardware consists of a limited amount of experience with no failures, as is generally the case for launch vehicle propulsion systems including those of the Space Shuttle, the data is a weak information source for failure risk assessment. However, measurements of physical parameters used in engineering analysis, such as temperatures and loads, can be a strong information source in failure risk estimation.

The failure risk estimate resulting from the combination of the prior risk estimate and the success/failure data is that which is warranted by the available information. As additional information regarding governing physical parameters becomes available, it can be incorporated into the engineering analysis to obtain revised prior failure risk estimates. Additional information in the form of success/failure data can be processed by the Bayesian statistical algorithm to update the failure risk estimate.

If the available success/failure data is a weak information source, the failure risk estimate will be predominantly determined by the prior failure risk estimate of Fig. 1. In such cases, the prior distributions must correctly represent the states of knowledge regarding risk of occurrence of the failure modes characterized by engineering analyses. It has been found in several case studies of SSME failure modes that incomplete knowledge of certain governing parameters in the engineering analyses is a major source of uncertainty in assessing the risk of occurrence of specific failure modes [7-12].

Probabilistic Failure Assessment

Approach and Structure

A formal stochastic structure for quantitatively assessing failure risk based on the available information about certain failure modes identified in a FMEA is shown in Fig. 2. Such a failure risk evaluation that considers failure modes meeting criteria discussed above is the foundation for assessing flight readiness. This stochastic structure is called the Probabilistic Failure Assessment (PFA) methodology and is an implementation of the Bayesian statistical framework described above in which information from engineering analysis is combined with success/failure data to obtain a quantitative failure risk estimate and a measure of its uncertainty [4]. The available information pertinent to characterizing specific failure modes is used in the PFA methodology not only to estimate the failure probability appropriate to the states of knowledge about failure modes, but also to characterize the sensitivity of failure probability to increased knowledge of such parameters as structural loads, operating environment, and materials behavior.

The elements presented in Fig. 2 are essential to evaluate failure risk rationally. These essential elements are: (1) the joint inclusion of information generated by engineering analysis and operating experience, (2) quantitative modeling of the physics and mechanics of the failure phenomenon, (3) representation of the uncertainty in the engineering analysis parameters and models, including uncertainty due to both intrinsic variation and lack of knowledge, and (4) consideration of multiple mission usage of flight systems.
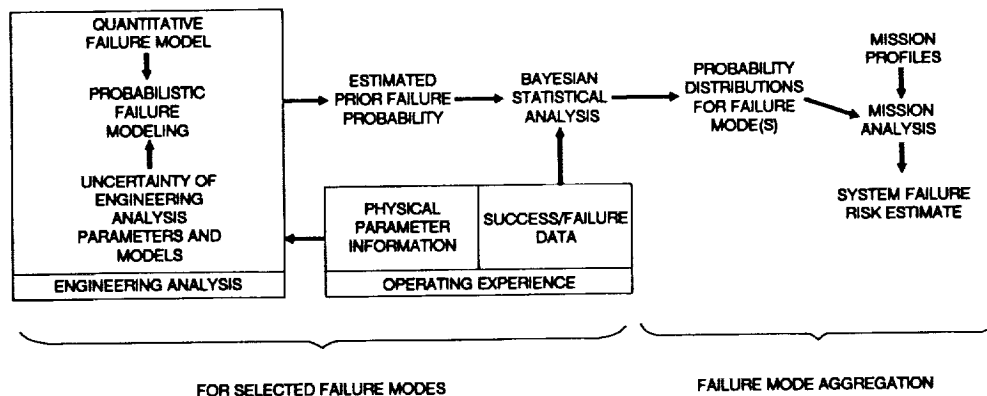

Figure 2. The Probabilistic Failure Assessment Methodology

The PFA methodology consists of three major steps: probabilistic failure modeling, a Bayesian statistical analysis to consider the available success/failure data, and a mission analysis in which the failure estimates for a number of relevant failure modes are aggregated to obtain a system failure risk estimate for the service life. Probabilistic failure modeling and the Bayesian statistical analysis are performed for each failure mode identified for analysis.

The PFA methodology employs the quantitative models used in engineering analyses of failure modes in a probabilistic structure within which uncertainties due to limited information regarding values for analysis parameters and the accuracy of the models employed are quantitatively treated. The stochastic structure and statistical approach are generally applicable to failure modes of spaceflight systems. The PFA methodology may be applied to any failure

5

mode for which quantitative engineering analysis can be employed to characterize the failure phenomenon.

Probabilistic Failure Modeling

The probabilistic failure modeling step of the PFA methodology is shown in greater detail in Fig. 3. In this step, uncertainties in engineering analysis parameters and models for the failure mode being analyzed are used in conjunction with the quantitative model of the failure phenomenon to simulate failures. The failure models are directly derived from the engineering analyses of the failure mode and express a failure parameter, such as burst pressure or fatigue life, as a function of *drivers*. The drivers include dimensions, loads, materials characteristics, modeling accuracy, and environmental parameters such as local temperatures.

For many important failure modes, the failure model of Fig. 3 is complex and involves the use of several engineering analysis procedures. The accuracy of each engineering model and procedure is probabilistically characterized and also treated as a driver in the PFA methodology. A typical stochastic materials characterization model is discussed in [9]. In that model both the intrinsic variability of materials behavior and the uncertainty resulting from basing a model of that behavior on limited information are treated.

State-of-the-art engineering models of failure modes used by the National Aeronautics and Space Administration (NASA) and the launch vehicle propulsion system manufacturers incorporate procedures that have evolved through extensive experience. These deterministic models are comprised of a series of steps, each of which may be complex. The PFA methodology has been developed to accommodate generally accepted engineering models in current use. Assessments of model accuracy are based on an organization's experience with these engineering models and on specific calibrations of the models.
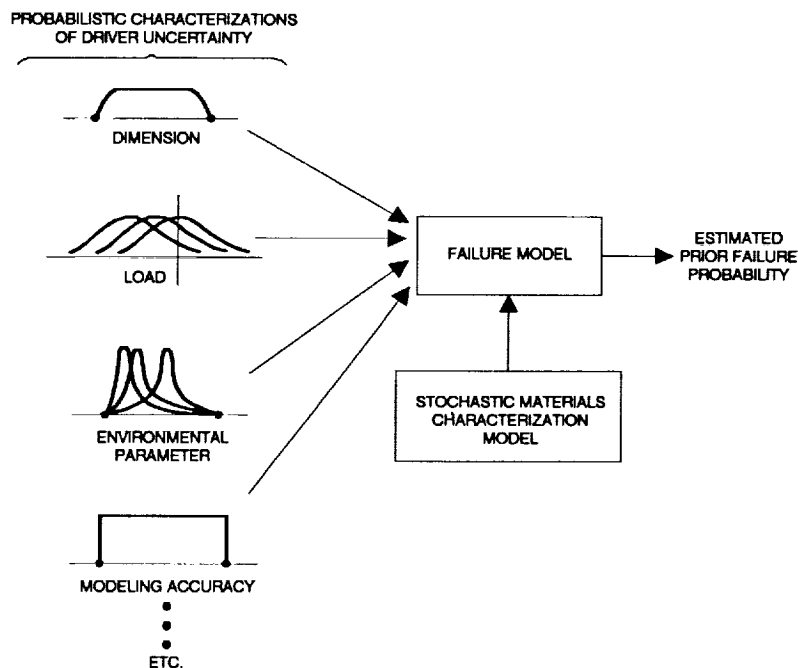

Figure 3. The Probabilistic Failure Modeling Procedure

6

By calculating failure risk from an analysis based on the specification of failure models and drivers, the PFA methodology permits the quantitative assessment of failure risk when the failure data necessary to characterize component reliability does not exist.

Driver Characterization

In the PFA methodology, a driver for which uncertainty is to be considered is characterized by a probability distribution over the range of values it can assume. That distribution expresses uncertainty regarding specific driver values within the range of possible values. A driver probability distribution must represent both intrinsic variability of the driver and uncertainty due to limited information on which to base the driver characterization. There is no restriction on specifying explicit driver probability distributions or defining processes which generate implicit driver probability distributions.

Stochastic drivers are characterized by using the information that exists at the time of analysis. If driver information is sparse, then the probabilistic characterization of such a driver must reflect that sparseness. If extensive experimental measurements have been performed for a driver, its nominal value and characterization of its variability can be inferred directly from empirical data. However, if little or no directly applicable empirical data is available for a driver, engineering analysis and past experience with similar or related systems must be used instead.

The information on which driver characterization is based can include measurements, related past experience, and engineering analysis conducted to bound or characterize the driver. All sources of driver uncertainty must be considered to appropriately represent risk due to limited information, and driver distributions must meet the criterion of not overstating the available information. Drivers are fundamental in the sense that they are observable parameters for which additional information regarding their values can be obtained if necessary. Such parameters include temperatures, loads, materials behavior, and calibrations of model accuracy. If uncertainty due to lack of information on a driver is found to make a significant contribution to failure risk, then additional driver information should be acquired.

Computational Methods

The complexity of failure models and the need for a computational procedure capable of accuracy have led to the use of Monte Carlo simulation as the principal computational method in the probabilistic failure modeling step of Fig. 2. Monte Carlo simulation is a general method for probabilistic analysis that can be used with failure models of any complexity. Continually increasing computer power due to improving hardware and software is steadily expanding the practical application of such computationally intensive methods as Monte Carlo simulation. Efficient Monte Carlo techniques are available to reduce the number of simulation trials for those problems where computational time would be an issue if direct Monte Carlo simulation were used.

Alternatives to Monte Carlo methods may fail to give demonstrably accurate results for realistic problems in which complex failure models are employed. Alternative computational methods can be used in probabilistic analyses which employ well-behaved failure models, particularly if the failure criterion is expressed explicitly in a closed form equation as opposed to a complex multistep algorithm.

Certain engineering analysis procedures sometimes employed in failure models, such as finite-element structural models, may appear to be too computationally intensive for practical use in a Monte Carlo simulation. However, when such procedures are used in a failure model for PFA, they can be represented as response surfaces over the range of variation of significant parameters. Alternative computational techniques may be useful in conducting engineering analyses to generate such response surfaces. The uncertainties of engineering analysis procedures and of the response surface representation must be treated as drivers if significant.

Application of Probabilistic Failure Assessment

In assessing flight readiness, sound judgment is required to identify critical failure modes, to understand their origins and mechanisms, and to guide the implementation of the probabilistic analysis. The failure models required for meaningful probabilistic analysis must be developed in concert with a valid interpretation of relevant experience. Adjudging failure probabilities, even with the most sophisticated methods, does not imply that the origins, mechanisms, and consequences of known failure modes are understood and have been properly treated nor that unexpected test observations and indications of unanticipated failure modes have been pursued until they are understood and accounted for. An understanding of the causes and mechanisms by which failures occur is the foundation on which valid failure models must be based.

The necessity for conducting an appropriate amount of testing for launch vehicle propulsion systems is not eliminated through the use of the PFA methodology to assess risk of failure. Testing programs and careful analysis of flight experience are essential because they can uncover failure modes not analyzed, analysis oversights or errors, and anomalous conditions.

Application of the PFA methodology to a subset of failure modes selected by a FMEA and other screening procedures will identify those failure modes whose risk of occurrence is unacceptable. Options for corrective action that could be taken to reduce risk are shown in Fig. 4. Since the PFA methodology produces a risk assessment that is commensurate with the available information, an unacceptable risk could be reduced by acquiring additional informa-
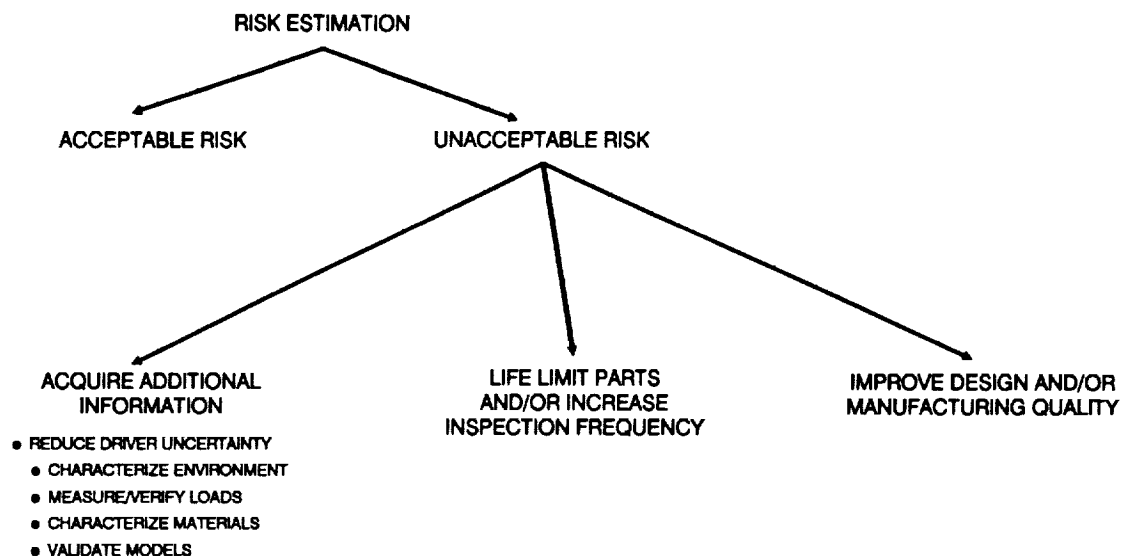

Figure 4. Options for Reducing Failure Risk

8

tion to reduce the uncertainty of dominant drivers or by changing the design so that the available information is sufficient.

By conducting sensitivity analyses for selected failure modes with the PFA methodology, the sources of unacceptable failure risk can be identified in terms of the responsible drivers, and corrective action can be delineated. Improvements in manufacturing processes, additional characterization of loads and environments, validation of analytical models, improved characterization of materials behavior, design changes, and additional testing are among the options for corrective action that can be quantitatively evaluated by PFA sensitivity analyses. The PFA methodology can be employed to identify risk sources and corrective actions during the design, development, and operational phases of a program.

Risk assessments for critical failure modes of SSME components both in use and in development have been conducted by means of the PFA methodology and are documented in [7-12]. These case studies demonstrate the techniques of the PFA methodology and illustrate its use to quantify failure risk and to identify the dominant drivers that contribute to risk.

Conclusions

The PFA methodology is a structured, probabilistic approach for quantitatively assessing the risk of occurrence of critical failure modes identified by a FMEA and other screening procedures. Whenever flight readiness must be assured under conditions of limited information and uncertain knowledge that are typical of launch vehicle propulsion systems, including those of the Space Shuttle, no other rational approach for quantitatively assessing and managing failure risk is available. The PFA methodology provides the capability to quantitatively evaluate and rank options to improve reliability, thereby enabling limited financial resources for development and improvement programs to be more effectively allocated. In particular, the PFA methodology provides a means for basing the certification of flight readiness on a quantitative assessment of failure risk.

References

[1] Feynman, R. P., "Personal Observations on Reliability of Shuttle," *Report of the Presidential Commission on the Space Shuttle Challenger Accident*, Appendix F, 1986.

[2] "Post Challenger Evaluation of Space Shuttle Risk Assessment and Management," Committee on Shuttle Criticality Review and Hazards Analysis Audit, National Research Council, Washington, D.C., 1988.

[3] Moore, N., et al., *A Review of Certification Practices Potentially Applicable to Man-Rated Reusable Rocket Engines - Certification Process Assessment Task*, JPL D-7969, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California, February, 1986 (internal document).

[4] Moore, N., Ebbeler, D., and Creager, M., "A Methodology for Probabilistic Prediction of Structural Failures of Launch Vehicle Propulsion Systems," *Proceedings of the AIAA/ASME/ASCE/AHS/ASC 31st Annual Structures, Structural Dynamics, and Materials Conference*, 1990, part 2, pp. 1092-1104.

[5] Federal Aviation Regulation, Part 33, Section 33.14, Amendment 33-6, 1974.

[6] Martz, H. F., and Waller, R. A., *Bayesian Reliability Analysis*, John Wiley & Sons, New York, N.Y., 1982.

[7] Newlin, L., et al., "Probabilistic Low Cycle Fatigue Failure Analysis Applicable to Liquid Propellant Rocket Engines," *Proceedings of the AIAA/ASME/ASCE/AHS/ASC 31st Annual Structures, Structural Dynamics, and Materials Conference*, 1990, part 2, pp. 1115-1123.

[8] Sutharshana, S., et al., "Probabilistic High Cycle Fatigue Failure Analysis Applicable to Liquid Propellant Rocket Engines," *Proceedings of the AIAA/ASME/ASCE/AHS/ASC 31st Annual Structures, Structural Dynamics, and Materials Conference*, 1990, part 2, pp. 1105-1114.

[9] Moore, N., et al., *An Improved Approach for Flight Readiness Certification - Methodology for Failure Risk Assessment and Fatigue Failure Mode Case Study Examples*, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California, review draft distributed October, 1989 (forthcoming).

[10] Sutharshana, S., et al., "A Probabilistic Fracture Mechanics Approach for Structural Reliability Assessment of Space Flight Systems," submitted for ASTM Special Technical Publication *Advances in Fatigue Lifetime Predictive Techniques*, February, 1990.

[11] *Status Review - Certification Process Assessment Task*, JPL D-6884, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California, November 14, 1988 (internal document).

[12] *Status Review - Certification Process Assessment Task*, JPL D-6883, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California, September 22, 1987 (internal document).

1. Report No. JPL-Pub-90-46	2. Government Accession No.	3. Recipient's Catalog No.

4. Title and Subtitle	5. Report Date October 30, 1990
An Improved Approach for Flight Readiness Assessment	6. Performing Organization Code

7. Author(s) N. R. Moore, D. H. Ebbeler, and M. Creager	8. Performing Organization Report No.

9. Performing Organization Name and Address	10. Work Unit No.
JET PROPULSION LABORATORY California Institute of Technology 4800 Oak Grove Drive Pasadena, California 91109	11. Contract or Grant No. NAS7-918
	13. Type of Report and Period Covered JPL Publication

12. Sponsoring Agency Name and Address	
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION Washington, D.C. 20546	14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

An improved methodology for quantitatively evaluating failure risk for a spaceflight system in order to assess flight readiness is presented. This methodology is of particular value when information relevant to failure prediction, including test experience and knowledge of parameters used in engineering analyses of failure phenomena, is limited. In this approach, engineering analysis models that characterize specific failure modes based on the physics and mechanics of the failure phenomena are used in a prescribed probablistic structure to generate a failure probability distribution that is modified by test and flight experience in a Bayesian statistical procedure. The probablistic structure and statistical methodology are generally applicable to any failure mode for which quantitative engineering analysis can be employed to characterize the failure phenomenon and are particularly well suited for use under the constraints on information availability that are typical of such apceflight systems as the Space Shuttle and planetary spacecraft.

17. Key Words (Selected by Author(s))	18. Distribution Statement
Spacecraft Design, Testing, and Performance. Quality Assurance and Reliability Structural Engineering Reliability	Unclassified, Unlimited

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 10	22. Price